UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/780,848	02/18/2004	Michael Thomas Kurdziel	RF-235 (50589)	2513

74701 7590 03/05/2009

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST
255 S ORANGE AVENUE
SUITE 1401
ORLANDO, FL 32801

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
03/05/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

creganoa@addmg.com

Office Action Summary	Application No.	Applicant(s)	
	10/780,848	KURDZIEL ET AL.	
	Examiner	Art Unit	
	ABDULHAKIM NOBAHAR	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 October 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-12,14-21 and 23-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-12,14-21 and 23-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's amendment filed on 10/15/2008.

2. Claims 1-4, 6-12, 13-21 and 23-26 are pending.

3. Claims 5, 13 and 22 are cancelled.

4. Claims 1, 6, 10, 14, 18 and 23 are amended.

5. Applicant's arguments with respect to the claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-12, 13-21 and 23-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al (6,769,063 B1) hereinafter Kanda in view of Stein et al (US 2003/0133568 A1) hereinafter Stein.

In reference to claims 1, 10 and 18, Kanda discloses:

a cryptographic device (see Figs. 1 and 4) comprising:

a key scheduler providing a key data block comprising a plurality of sub-key data blocks (see Fig. 1, and Fig. 4, block 20); and

An input stage receiving an input data block (see Fig. 1, 64; Fig. 2, block 17; Fig. 4, block 301; Fig. 5, block 341) and a key data block comprising a plurality of sub-key data blocks (see Fig. 1, master key, block 21 and K0, K1…K15; col. 9, lines 21-27; Fig. 4, blocks 320-322), and generating a plurality of first signals therefrom, that are in parallel based upon the input data block and a key data block (see Fig. 2, where a plurality of subkeys 6 are generated from the input data block R1 and key block of K1; Fig. 5, in0-in3).

An intermediate stage connected to said input stage (see Fig. 2, S-boxes S0-S7; Fig. 5, blocks 343s and 345s) and comprising

A plurality of substitution units operating in parallel, each substituting data within a respective first signal (see col. 2, lines 22-39; Fig. 2, S-boxes S0-S7; Fig. 5, blocks non-linear transformation parts 343s and 345s), and

A diffuser connected to said plurality of substitution units for mixing data to generate a diffused signal (see Fig. 2, S-boxes S0-S7; Fig. 5, block 346, where the combining part 346 and signal 32 correspond to the recited diffuser and diffused signal, respectively),

An output stage connected to said intermediate stage for repetitively looping back the diffused signal to said input stage for combination with a next sub-key data block (see col. 1, lines 42-67; Fig. 4, where every round processing part 38 provide an output to the next one to be combined with the another subkey in the non-linear function part and the round processing corresponds to the recited repetitively looping back; col. 9, lines 4-20; Fig. 13, where each round has an output part similar to the output part 309),

Kanda, however, does not expressly disclose that said diffuser comprising at least one shift register and at least one look-up table associated therewith

Stein discloses an improved programmable data encryption engine for performing the cipher function of an advanced encryption standard (AES) using the Rijndael algorithm (see Summary). Stein further discloses that based on the AES algorithm the data block undergoes transformation in the S-BOX and then a shift row (corresponds to the recited shift register) transformation followed by a mix column transformation (see Fig. 2 and [0031]). The combination of shift row transformation and mix column transformation operations that are carried out after S-BOX transformation operation corresponds (or it is functionally equivalent) to the recited diffuser section of the intermediate stage of the instant invention. Furthermore, Stein discloses that its invention in one embodiment has a parallel look-up table for performing the shift row transformation in addition to the parallel look-up table for S-BOX transformation (see [0033]). Thus, Stein discloses a system that has a section (i.e. a stage) that perform shift row and mix column transformations which includes a look-up table corresponding to the diffuser recited in claims 1, 10 and 18. It would have been obvious to a person of ordinary skill in the art at the time of the invention was made to implement a data encryption scheme performing the cipher function of AES algorithm as taught in Stein in the system of Kanda because it would make the system of Kanda significantly faster (see Stein, [0009]).

In reference to claims 2 and 19, Kanda discloses:

a cryptographic device according to claim 1 wherein the looping back is repeated a predetermined number of times; and wherein said output stage provides an output signal for the cryptographic device after the repetitively looping back is complete (see col. 9, lines 4-20, where N specifies the number rounds or the number of times that the non-linear processing is repeated and col. 9, lines 64-67).

In reference to claims 3, 11 and 20, Kanda discloses:
a cryptographic device according to claim 2 wherein the output signal is further combined with a final sub-key data block (see Fig. 13, block 308).

In reference to claims 4, 12 and 21, Kanda discloses:
a cryptographic device according to Claim 1 wherein each substitution unit performs a non-linear substitution based upon at least one look-up table (see col. 2, lines 31-34; Fig. 13, block 304).

In reference to claims 6, 14 and 23, Kanda in view of Stein discloses:
wherein said at least one shift register comprises a plurality of shift registers and said at least one look-up table comprises a plurality of look-up tables associated therewith (see Kanda, col. 13, line 63-col. 14, line 28, where the logical linear operations correspond to the recited shift register; Stein, [0012], where the parallel look-up table system may include a memory, a plurality of look-up tables...and [0035], where the system include three registers).

In reference to claims 7, 15 and 24, Kanda discloses:

a cryptographic device according to claim 1 wherein said output stage performs a row-shift operation on the diffused output signal before being looped back to said input stage (see col. 9, lines 36-40, where the bit rotation corresponds to the recited row-shift operation and col. 13, line 63-col. 14, line 28, where the bit rotation corresponds to the recited row-shift register).

In reference to claims 8, 16 and 25, Kanda discloses:

a cryptographic device according to claim 1 wherein said output stage performs a column-mix operation on the diffused output signal being looped back to said input stage (see col. 12, lines 31-45; col. 13, lines 37-41).

In reference to claims 9, 17 and 26, Kanda discloses:

A cryptographic device according to Claim 1 wherein said output stage comprises a counter for counting a number of times the diffused output signal is looped back to said input stage (see col. 9, lines 64-37; Fig. 11, step S7).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ABDULHAKIM NOBAHAR whose telephone number is (571)272-3808. The examiner can normally be reached on M-T 8-6.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Abdulhakim Nobahar/
Examiner, Art Unit 2432

February 27, 2009